**Title:** Bezpieczeństwo danych i systemów informacyjnych w bibliotekach. Przegląd stanu prawnego

**Author:** Andrzej Koziara, Agnieszka Jezierska

**Citation style:** Koziara Andrzej, Jezierska Agnieszka. (2015). Bezpieczeństwo danych i systemów informacyjnych w bibliotekach. Przegląd stanu prawnego. "Bibliotheca Nostra. Śląski Kwartalnik Naukowy" (2015, nr 4, s. 41-53).

Bibliotheca Nostra.
Śląski Kwartalnik Naukowy
nr 4 (42) 2015, s. 41-53

Andrzej Koziara
*Biblioteka Uniwersytetu Śląskiego w Katowicach*

Agnieszka Jezierska
*Uniwersytet Śląski w Katowicach, Dział Audytu*

# Bezpieczeństwo danych i systemów informacyjnych w bibliotekach. Przegląd stanu prawnego

Biblioteka, nie tylko naukowa, jak każda instytucja działająca w drugiej dekadzie XXI w. wymaga szeroko pojętego wspomagania systemami teleinformatycznymi. Zakres wspomagania zależny jest od gamy świadczonych usług informacyjno-bibliotecznych, natomiast zasady budowy takich systemów wyznaczają czynniki techniczne, powiązane z obecnym poziomem technologii jak również aktualnym stanem rozwiązań prawnych i normatywnych.

Dla zrozumienia związków systemowych pomiędzy poszczególnymi elementami tworzonego systemu bezpieczeństwa informacji niezbędne jest określenie, czym jest samo bezpieczeństwo. Kreśląc, na potrzeby niniejszego artykułu, obraz bezpieczeństwa należy zwrócić uwagę na jego dwa aspekty. Pierwszy z nich wynika z faktu, że bezpieczeństwo to jeden z najważniejszych elementów opisujących instytucję i w sposób znaczący wpływających na poziom wykonywanych przez nią, zgodnie z prawem, usług informacyjno-bibliotecznych. Drugi aspekt odnosi się do ustalenia, że zapewnienie bezpieczeństwa to zestaw działań mających na celu taką organizację instytucji, by wszystkie prowadzone przez nią działania były zgodne z prawem, jej statutem i regulaminami, zapewniając równocześnie zadowalający poziom satysfakcji użytkowników. Przeprowadzone studia literaturowe wskazują, że w dotychczasowych badaniach porządkujących sprawę ochrony informacji traktowano ją wyrywkowo – zajmowano się osobno danymi osobowymi, informacją publiczną czy informacjami ustawowo chronionymi, bardzo często zawężając obszar badawczy do szczegółowych działów działalności administracyjnej[1]. Przygotowujący opracowania

[1] Zagadnienia ochrony informacji najczęściej są poruszane w programach szkoleń, prezentacjach zamieszczanych w wolnych źródłach publikacyjnych oraz na łamach czasopisma „Informacja w Administracji Publicznej" – ISSN 2392-2265. Pomocą źródłową służą portale: International Electrotechnical Commission (http://www.iec.ch/), International Organization

praktycznie skupiali się na zagadnieniach szczegółowych, wynikających z pojedynczych aktów prawnych, uzupełniając je o omówienia, w których odnoszą się do uzupełniających je rozporządzeń lub innych ściśle powiązanych z nimi aktów prawnych. Było to jedynie fragmentaryczne spojrzenie na całość informacji, w której wyróżniano pewne grupy zagadnień, niekoniecznie najważniejsze dla działalności biznesowej instytucji, lecz w sposób sztuczny wydzielone przez szczegółowe przepisy prawa.

Opracowanie niniejsze stanowi próbę wyspecyfikowania i uporządkowania wszystkich obowiązujących w pierwszej połowie 2015 r. przepisów i norm, które powinny być uwzględniane przy tworzeniu systemu bezpieczeństwa informacji dla bibliotek naukowych publicznych szkół wyższych. Należy zwrócić uwagę, że sprawa bezpieczeństwa informacji nie może być traktowana w bibliotekach jako element tymczasowy lub tylko wycinkowy, potrzebny np. do prowadzenia punktów informacji normalizacyjnych, działających na podstawie umów z Polskim Komitetem Normalizacyjnym. Zastosowana metodyka może posłużyć jako przykład do przygotowania podobnych opracowań dla innych instytucji publicznych lub organów administracji samorządowej. Charakterystyki takie są wstępem do przeprowadzenia szczegółowych analiz służących wdrażaniu rozwiązań zapewniających kompleksowe bezpieczeństwo informacji. Prace zmierzające do zapewnienia akceptowalnego poziomu bezpieczeństwa informacji można prowadzić efektywnie, gdy działania są oparte o systemy jakościowe, co w uproszeniu można interpretować jako wdrażanie standardów zarządzania poprzez jakość[2], wpływające w przypadku bibliotek szkół wyższych na jakość świadczonych usług informacyjno-bibliotecznych.

Przed przystąpieniem do porządkowania i wartościowania aktów normatywnych, celowe jest podjęcie intuicyjnych prac zmierzających do zinwentaryzowania sfer, w których niezbędne wydają się działania związane z ochroną informacji. Ich istotą jest uświadomienie, w szczególności kadrze zarządzającej, że zapewnienie bezpieczeństwa informacji nie jest problemem pionów informatycznych lecz całej instytucji. Do najbardziej typowych obszarów dotyczących działań związanych z zapewnieniem bezpieczeństwa należą:

- tradycyjne zbiory danych (głównie papierowe);
- zbiory danych w pracujących systemach teleinformatycznych;
- system archiwizacji danych i nośniki, na których przechowywane są dane;

for Standardization (http://www.iso.org), Polski Komitet Normalizacyjny (http://pkn.pl) oraz baza danych Lex Omega.

[2] Wnioski wynikające z konferencji naukowej podsumowującej realizację projektu Tempus UM JEP 13242-98 „Modernizacja zarządzania biblioteką jako część zarządzania przez jakość w Uczelni – cele i zadania" (Derfert-Wolf, Bednarek-Michalska, red., 2000).

- systemy zabezpieczeń fizycznych;
- procedury postępowania.

Analizując zakres wyspecyfikowanych pól, należy zauważyć, że odnoszą się do wszystkich elementów działalności statutowej bibliotek, a niewłaściwe zorganizowanie pracy instytucji może hipotetycznie grozić nawet utratą ciągłości działania.

Na wstępie, korzystając z zasad racjonalnego zarządzania instytucją publiczną, należy dokonać inwentaryzacji aktów, których stosowanie staje się niezbędne dla zachowania zgodności z aktualnym stanem prawnym. W zakresie zapewnienia bezpieczeństwa informacji są to:

1. Ustawy;
2. Rozporządzenia Rady Ministrów, Prezesa Rady Ministrów lub innych ustawowo upoważnionych ministrów;
3. Dyrektywy unijne i rozporządzenia Komisji (UE);
4. Normy międzynarodowe (najczęściej z ich implementacjami krajowymi);
5. Normatywne akty lokalne np. dla Biblioteki Uniwersytetu Śląskiego (BUŚ) – uchwały Senatu UŚ, zarządzenia JM Rektora UŚ czy zarządzenia Dyrektora Biblioteki UŚ[3].

**Ustawy**

W ramach aktualnie obowiązujących ustaw powinniśmy wskazać zarówno te, których stosowanie wynika bezpośrednio z przynależności organizacyjnej czy charakteru biblioteki, jak również związane z charakterem realizowanych przez bibliotekę usług informacyjno-bibliotecznych. W grupie ustaw podstawowych należy uwzględnić[4]:

- Ustawę z dnia 27 czerwca 1997 r. o bibliotekach (z późn. zm.); tekst jednolity na dzień 22 maja 2012 r. (Dz.U. 2012, poz. 642);
- Ustawę z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (z późn. zm.); tekst jednolity na dzień 9 października 2013 r. (Dz.U. 2014, poz. 1198);
- Ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (z późn. zm.); tekst jednolity na dzień 26 czerwca 2014 r. (Dz.U. 2014, poz. 1182);
- Ustawę z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (z późn. zm.); tekst jednolity na dzień 17 maja 2006 r. (Dz.U. 2006, nr 90, poz.631);
- Ustawę z dnia 27 lipca 2001 r. o ochronie baz danych (Dz.U. 2001, nr 128, poz.1402).

[3] Prezentowany stan prawny na dzień 28 lutego 2015 r.
[4] Analizę wykonano na dzień 1 stycznia 2015 r.

Pierwsza z wymienionych wyżej ustaw to akt ogólny regulujący pracę wszystkich bibliotek na terenie Rzeczypospolitej Polskiej. Jej art. 4 ust. 4 pkt 2 stanowi, że jest to „obsługa użytkowników, przede wszystkim udostępnianie zbiorów oraz prowadzenie działalności informacyjnej, zwłaszcza informowanie o zbiorach własnych" (Ustawa, 1997a). Taki opis realizowanych przez książnice zadań w połączeniu z powszechnym zastosowaniem do ich wspomagania systemów teleinformatycznych nakłada wraz z innymi aktami prawnymi konieczność chronienia wszystkich tworzonych w bibliotekach informacji. Dotyczy to nie tylko informacji o zbiorach własnych lecz wszystkich, które zostają wytworzone np. w czasie prowadzonych kwerend bibliotecznych. Natomiast ustawa Prawo o szkolnictwie wyższym, oprócz ogólnego tła normującego całościowe działania szkół wyższych, zawiera bardzo ważny art. 88 określający m.in. zasady przetwarzania danych osobowych gromadzonych w bibliotekach szkół wyższych (Ustawa, 2005). Szczególnie ważne są zapisy:

- ust. 4. mówiący, że „Uczelnia w związku z funkcjonowaniem systemu biblioteczno-informacyjnego może przetwarzać określone w jej statucie dane osobowe osób korzystających z tego systemu" (Ustawa, 2005) oraz
- ust. 5. mówiący, że: „Zbiór danych osobowych, o których mowa w ust. 4, jest zwolniony z obowiązku rejestracji zbiorów danych osobowych, o których mowa w art. 40 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych" (Ustawa, 1997b).

Są one uzupełnieniem postanowień wspomnianej wcześniej ustawy o ochronie danych osobowych. Dopełniają ją regulacje w zakresie prawa autorskiego i praw pokrewnych oraz ochrony baz danych. Szczególnej uwagi wymaga zwłaszcza ustawa o ochronie baz danych, gdyż najczęściej brak nam doświadczenia w jej stosowaniu. Najważniejszy dla praktyki bibliotecznej jest jej art. 7 ust. 1 mówiący, że „Producent bazy danych udostępnionej publicznie w jakikolwiek sposób nie może zabronić użytkownikowi korzystającemu zgodnie z prawem z takiej bazy danych, pobierania lub wtórnego wykorzystania w jakimkolwiek celu nieistotnej, co do jakości lub ilości, części jej zawartości", a także uregulowanie zgodnie z jej art. 8 mówiące że „Wolno korzystać z istotnej, co do jakości lub ilości, części rozpowszechnionej bazy danych", gdy realizujemy to do własnego użytku osobistego, ale tylko „z zawartości nieelektronicznej bazy danych" oraz bez określania zakresu „w charakterze ilustracji, w celach dydaktycznych lub badawczych, ze wskazaniem źródła, jeżeli takie korzystanie jest uzasadnione niekomercyjnym celem, dla którego wykorzystano bazę" (Ustawa, 2001). Sformułowania te w sposób oczywisty uzupełniają zawarte w ustawie o prawie autorskim postanowienia dotyczące publikacji nie będących bazami danych.

Pamiętając, że działalność biblioteki jest prowadzona wielopłaszczyznowo, podczas przygotowywania dokumentów związanych z bezpie-

czeństwem informacji powinniśmy jeszcze uwzględnić akty prawne takie jak[5]:

- Ustawa z dnia 30 czerwca 2000 r. prawo własności przemysłowej (z późn. zm.); tekst jednolity na dzień 17 września 2013 r. (Dz.U. 2013, poz. 1410);
- Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (z późn. zm.); tekst jednolity na dzień 14 kwietnia 2014 r. (Dz.U. 2014, poz. 782);
- Ustawa z dnia 16 lipca 2004 r. prawo telekomunikacyjne (z późn. zm.); tekst jednolity na dzień 10 stycznia 2014 r. ( Dz.U. 2014, poz. 243);
- Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną; tekst jednolity na dzień 15 października 2013 r. (Dz.U. 2013, poz. 1422);
- Ustawa z dnia 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym (Dz.U. 2002, nr 126, poz. 1068 z późn. zm.).

Ustawy te, mimo że pozornie nie mają wpływu na organizację pracy biblioteki, w rzeczywistości mogą jednak oddziaływać na niektóre elementy jej funkcjonowania. Szczególnie może to dotyczyć sytuacji związanych z udostępnianiem informacji patentowej i pokrewnej lub informacji wykorzystywanej podczas tworzenia Biuletynów Informacji Publicznej, a także wdrażania innowacyjnych technologii informacyjnych, wspomaganych nowoczesnymi systemami teleinformatycznymi. Dodatkowym zagadnieniem, leżącym w sferze zainteresowań bibliotek, jest ich udział we wtórnym rozpowszechnianiu informacji publicznej. Niejednokrotnie, mimo że postanowienia wspomnianych ustaw nie mają zastosowania wprost, treści w nich zawarte są w dużym zakresie pomocne przy przygotowaniu i wdrażaniu systemów bezpieczeństwa.

**Rozporządzenia**

Kolejną grupę stanowią akty wydawane przez Radę Ministrów opublikowane w Dzienniku Ustaw, w Monitorze Polskim czy dziennikach resortowych. Do najważniejszych należą:

W zakresie ogólnym:

- Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych zwanego w dalszej części tekstu „w sprawie KRI" (Dz.U. 2012, poz. 526) ze zmianami opubli-

[5] Analizę wykonano na dzień 1 stycznia 2015 r.

kowanymi w dniu 1 grudnia 2014 r. (Dz.U. 2014, poz. 1671) zastępujące po ponad dwuletniej luce legislacyjnej obowiązujące wcześniej dwa rozporządzenia w sprawie minimalnych wymagania dla rejestrów publicznych i wymiany informacji w formie elektronicznej (Dz.U. 2005, nr 214, poz. 1781) oraz w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2005, nr 212, poz. 1766).

W zakresie stosowania ustawy o ochronie danych osobowych:

- Na podstawie art. 39(a) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, opublikowane w dniu 1 maja 2004 r. (Dz.U. 2004, nr 100, poz. 1024)[6].
- Na podstawie art. 46(a) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. wzór zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, opublikowane w dniu 1 maja 2004 r. (Dz.U. 2004, nr 100, poz. 1025), zmienione obecnie przez rozporządzenie z dnia 11 grudnia 2008 r. (Dz.U. 2008, nr 229, poz. 1536).

Analizując zapisy, dostrzegamy, że dla rozporządzenia w sprawie KRI charakterystyczne jest bardzo poważne potraktowanie norm międzynarodowych dotyczących systemów bezpieczeństwa informatycznego, jako wzorca postępowania przez wszystkie instytucje publiczne (Rozporządzenie, 2012). Reformowany system normalizacyjny dotychczas traktował stosowanie norm w organizacji pracy instytucji w sposób uznaniowy. Normy te, mimo że zsynchronizowane z europejskim i światowym systemem, były postrzegane jako wzorce postępowania, które nie musiały być stosowane. Odmienne potraktowanie tego systemu w rozporządzeniu Rady Ministrów tworzy precedens pozwalający na wytworzenie kultury organizacyjnej opartej o rozwiązania normalizacyjne. Główne normy wymienione w tym rozporządzeniu to PN-ISO/IEC 27001, PN-ISO/IEC 17799, PN-ISO/IEC 27005 i PN-ISO/IEC 24762. Równocześnie ważnym obowiązkiem, który został nałożony tym zarządzeniem na instytucje eksploatujące systemy teleinformatyczne, jest przeprowadzanie audytu systemów teleinformatycznych oraz audytu ich bezpieczeństwa.

Omawiając rozporządzenia dotyczące bezpieczeństwa danych osobowych, należy poddać analizie rozporządzenie określające w sposób bardzo

[6] Uwaga: powszechnym błędem wskazywanym przez GIODO jest stosowanie nieobowiązującego Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. ze zmianą z dnia 1 października 2001 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

precyzyjny i praktyczny organizację bezpieczeństwa systemów przetwarzających dane osobowe jako modelu kompleksowej organizacji systemów bezpieczeństwa systemów teleinformatycznych instytucji. Wydaje się, że rozporządzenie to jako „wyciąg" z różnych norm teleinformatycznych jest dobrym startowym wzorcem do rozpoczęcia pracy nad budową systemu informacji.

Dla Biblioteki Uniwersytetu Śląskiego szczególne znaczenie miała pierwsza wersja rozporządzenia o rejestracji zbioru danych czytelników w GIODO[7], gdyż właśnie BUŚ jako jedna z nielicznych bibliotek szkół wyższych w zgłoszeniu z 2005 r. deklarowała wszystkie elementy, niezbędne do stworzenia elementarnego systemu bezpieczeństwa informacji. Już wówczas myślano tu o tworzeniu kompleksowych rozwiązań techniczno-organizacyjnych, które w swoim pierwszym etapie były oparte o rozwiązania opisywane w normach wydanych przez British Standards Institution (BSI) oraz pierwszych wersjach norm ISO. Tak prowadzone działania pokazywały odmienność podejścia do problemów bezpieczeństwa informacji w Uniwersytecie Śląskim, który podjął trud przemyślanego i kompleksowego wdrażania systemów informatycznych obsługujących w sposób centralny wszystkie procesy biznesowe uczelni (Koziara, Magiera, 2005). W czasie planowania tych rozwiązań projektowano również w sposób całościowy systemy bezpieczeństwa informacji, co pozwoliło sprostać wymaganiom wynikającym ze stosowania omawianych rozporządzeń i stworzyć wzorzec dla innych instytucji publicznych. Elementy te są cały czas udoskonalane i przystosowywane do zmieniających się wymagań.

**Dyrektywy Unijne i rozporządzenia Komisji Europejskiej**

Podejmują działania porządkujące oraz zapoznają z treściami prawodawstwa europejskiego. Należą do nich:

- Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U.UE.L. z dn. 23 listopada 1995 r., nr 1995.281.31;
- Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz.U.UE.L. z dn. 17 lipca 2000 r., nr 2000.178.1);
- Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywat-

[7] Opublikowana 1 maja 2004 r., w dniu akcesji Polski do Unii Europejskiej.

ności i łączności elektronicznej), (Dz.U.UE.L. z dn. 31 lipca 2002 r., nr 2002.201.37);

- Rozporządzenie (WE) Nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.U.UE.L. z dn. 12 stycznia 2001 r., nr 2001.8.1);
- Rozporządzenie Komisji (UE) NR 611/2013 z dnia 24 czerwca 2013 r. w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady o prywatności i łączności elektronicznej (Dz.U.UE.L. z dnia 26 czerwca 2013 r., nr 2013.173.2).

Przytoczone dyrektywy i rozporządzenia to najważniejsze dokumenty wspólnotowe, które stały się źródłem wybranych uregulowań polskiego prawodawstwa z zakresu ochrony różnego typu danych tworzonych wewnętrznie lub powierzanych do przetwarzania. Na mocy wymienionych dokumentów podejmowane są decyzje Komisji Europejskiej w sprawie szczegółowych rozwiązań w kwestii przekazywania danych osobowych do podmiotów trzecich. Dla obywateli państw członków Unii Europejskiej ma to szczególne znaczenie w sytuacji, gdy sprawa ochrony danych przekracza granice ich państw. Równocześnie treść wydawanych dyrektyw pozwala na planowanie działań wyprzedzających państwowe regulacje prawne. Jest to szczególnie cenne, gdy stosujemy normy w zakresie zarządzania jakością i bezpieczeństwem informacji oraz planujemy działania w trybie ciągłego doskonalenia jakości procedur. Walor wcześniejszego interpretowania zapisów jest bardzo ważny dla bibliotek – instytucji, których działalność opiera się na przygotowywanych i rozwijanych systemach teleinformatycznych, wspomagających cyrkulacje gromadzonych przez wiele lat zbiorów. Brak antycypacji zmian przepisów wynikających z wprowadzanych do prawodawstwa krajowego zapisów dokumentów europejskich może narazić wszystkie instytucje na ponoszenie dodatkowych, nieuzasadnionych z punktu widzenia dyscypliny finansów publicznych kosztów inwestycyjnych lub eksploatacyjnych.

**Normy międzynarodowe**

Normy w zakresie bezpieczeństwa systemów teleinformatycznych możemy podzielić na dwie grupy. Do pierwszej należą te, które w sposób porządkowy określają sposoby organizacji pracy instytucji niezbędne do zachowania bezpieczeństwa systemów informacyjnych. W drugiej zgrupowane są raporty przygotowane przez światowe służby techniczne. Za wydawanie norm międzynarodowych odpowiedzialna jest Międzynarodowa Organizacja Normalizacyjna ISO, znana pod angielską nazwą International

Organization for Standardization. Organizacja ta powstała po drugiej wojnie światowej, a wśród członków założycieli był Polski Komitet Normalizacyjny, który jest równocześnie wydawcą norm publikowanych w języku polskim. Konferencję, która dała początek działalności ISO, zwołano z inicjatywy BSI najstarszej na świecie działającej od początku XX w. instytucji zajmująca się tworzeniem norm. Trwające do dzisiaj wielkie zaangażowanie BSI w pracach ISO zaowocowało zastosowaniem zestawu norm BSI 7799 jako światowego wzorca norm bezpieczeństwa systemów informacyjnych. Dla norm technicznych dotyczących bezpieczeństwa organem przygotowującym takie raporty jest Międzynarodowa Komisja Elektrotechniczna (ang. International Electrotechnical Commission, IEC). Do najważniejszych norm z zakresu organizacji bezpieczeństwa informacji należą m.in. normy wymienione w Rozporządzeniu Rady Ministrów z roku 2012. Są to:

- PN-ISO/IEC 27001:2014-12 – wersja polska; Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania; Wprowadza: ISO/IEC 27001:2013 [IDT] zastępująca wymienioną w rozporządzeniu PN-ISO/IEC 27001:2007P wprowadzającą ISO/IEC 27001:2005 [IDT]);
- PN-ISO/IEC 27002:2014-12 – wersja polska; Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji; Wprowadza: ISO/IEC 27002:2013 [IDT] zastępująca wymienioną w rozporządzeniu PN-ISO/IEC 17799:2007P wprowadzającą ISO/IEC 17799:2005 [IDT];
- PN-ISO/IEC 27005:2014-01P; Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji; Wprowadza: ISO/IEC 27005:2011 [IDT] zastępująca wymienioną w rozporządzeniu PN-ISO/IEC 27005:2010 – wersja polska);
- PN-ISO/IEC 20000-1:2014-01P; Technika informatyczna – Zarządzanie usługami – Część 1: Wymagania dla systemu zarządzania usługami; Wprowadza: ISO/IEC 20000-1:2011 [IDT] zastępująca wymienioną w rozporządzeniu PN-ISO/IEC 20000-1:2007 - wersja polska, PN-ISO/IEC 20000-1:2007/Ap1:2008 – wersja polska;
- PN-ISO/IEC 20000-2:2007 – wersja polska; Technika informatyczna – Zarządzanie usługami – Część 2: Reguły postępowania; Wprowadza: ISO/IEC 20000-2:2005 [IDT] norma wymieniona w rozporządzeniu w tej chwili wycofana przez PKN lecz nie zastąpiona jeszcze wersją polską normy ISO/IEC 20000-2:2012 Information technology – Service management – Part 2: Guidance on the application of service management systems;
- PN-ISO/IEC 24762:2010 – wersja polska – Technika informatyczna – Techniki bezpieczeństwa – Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie – wprowadza ISO/IEC 24762:2008 [IDT] – wymieniona w dotąd nie zmienionej formie w rozporządzeniu.

Normami uzupełniającymi zasady stosowane w technikach teleinformatycznych jest rodzina norm – raportów technicznych oznaczona numerem 13335, które, mimo że były później zastępowane innymi dokumentami, niosą w sobie dużo informacji technologicznych. Należą do niej następujące polsko- i angielskojęzyczne dokumenty:

- PN-I-13335-1:1999P; Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych; Wprowadza: ISO/IEC/TR 13335-1:1996 [IDT] w wersji aktualnej jako anglojęzyczna występująca pod postacią dokumentu ISO/IEC 13335-1:2004 Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management;
- ISO/ IEC TR 13335-2 – opis planowania i zarządzania bezpieczeństwem systemów informatycznych w obecnej wersji aktualnej jako ISO/IEC TR 13335-2:1997 Information technology – Guidelines for the management of IT Security – Part 2: Managing and planning IT Security;
- ISO/ IEC TR 13335-3 – szczegółowy opis technik zarządzania bezpieczeństwem systemów informatycznych w tym trójpoziomowa polityka bezpieczeństwa w obecnej wersji aktualnej jako ISO/IEC TR 13335-3:1998 Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security;
- ISO/ IEC TR 13335-4 – zalecenia dotyczące doboru właściwego rodzaju zabezpieczeń w obecnej wersji aktualnej jako ISO/IEC TR 13335-4:2000 Information technology – Guidelines for the management of IT Security – Part 4: Selection of safeguards;
- ISO/ IEC TR 13335-5 – regulacje dot. zabezpieczeń połączeń z sieciami zewnętrznymi (sposoby zabezpieczania sieci wewnętrznej w miejscu jej połączenia z siecią zewnętrzną) w obecnej wersji aktualnej jako ISO/IEC TR 13335-5:2001 Information technology – Guidelines for the management of IT Security – Part 5: Management guidance on network security.

Normy te – w swym ówczesnym kształcie[8] – stały się podstawą rozporządzenia MSWiA w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Najważniejszymi zawartymi w nich uregulowaniami są: „sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych", „podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i sys-

[8] W postaci obowiązującej w kwietniu 2004 r.

temy informatyczne" oraz „wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych" (Rozporządzenie, 2004). Należy również pamiętać, że cała zawartość wymienionych powyżej norm to drogowskaz technologiczny, który powinien być elementarzem wymagań zarządzających instytucją wobec reguł postępowania opracowanych i wdrażanych w instytucji przez personel IT.

Nie można nie zauważyć, że na stan bezpieczeństwa wpływa ogólna organizacja firmy. Analizując najbardziej typowe środowisko instytucji, z dużym prawdopodobieństwem można przyjąć, że stan bezpieczeństwa zależy od działań wynikających z przyjętego systemu organizacyjnego, na który mają wpływ m.in. normy:

- PN-EN ISO 9001:2009P; Systemy zarządzania jakością – Wymagania, Wprowadza: EN ISO 9001:2008 [IDT];
- PN-N-19001:2006P; Wewnętrzny System Kontroli (WSK) – Wymagania – Uwaga nie wolno jej pomylić z normą PN-EN ISO 19001:2013-07;
- PN-N-18001:2004P; Systemy zarządzania bezpieczeństwem i higieną pracy – Wymagania.

Przytoczone powyżej normy z grupy PN-N to niemalże jednolite w skali europejskiej rozwiązania, które mają zapewnić kompatybilne dla firm środowiska pracy. Tak dla systemu kontroli jak i dla BHP jako podstawę przyjęto rozwiązania wynikające z normy 9001, przystosowując je do zadań związanych ze szczegółowym ich zastosowaniem.

Równocześnie nie wolno zapomnieć, że jednym z miękkich punktów przenikania zabezpieczeń jest nieautoryzowany dostęp fizyczny do samych urządzeń krytycznych, gdzie przechowywane są cenne dla nas dane. W związku z tym niezwykle ważne staje się stosowanie do zapisów z grupy norm PN-E-08390-XX:1993P lub 2000P; Rodziny norm: Systemy alarmowe, Włamaniowe systemy alarmowe.

**Prawo lokalne**

Jest to ostatnia grupa uregulowań prawnych, na które należy zwrócić uwagę. Może ona w swojej istocie być najbardziej pomocna we wdrażaniu zasad bezpieczeństwa systemów informacyjnych, lecz istnieje też potencjalne niebezpieczeństwo, że stanie się przeszkodą we właściwym przygotowaniu takiego systemu.

W przypadku Biblioteki Uniwersytetu Śląskiego są to:

- Statut Uniwersytetu Śląskiego – określenie zakresu danych osobowych przetwarzanych w systemie informatycznym BUŚ wyspecyfikowanym w rozdziale VI „System biblioteczno-informacyjny" § 42 pkt. 3;
- Zarządzenie nr 16/2014 Rektora Uniwersytetu Śląskiego w Katowicach z dnia 14 lutego 2014 r. w sprawie wprowadzenia do użytku służ-

bowego Polityki Bezpieczeństwa w Zakresie Ochrony Danych Osobowych w Uniwersytecie Śląskim oraz „Instrukcji Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych w Uniwersytecie Śląskim w Katowicach".

Reasumując. Przy przygotowaniu, wdrażaniu i utrzymaniu elementów systemu bezpieczeństwa niezbędne jest uwzględnienie wielu przepisów prawnych. Pomimo tego, że zbiór ich tworzy pozornie bardzo skomplikowane środowisko, według naszej oceny niemalże każdą z instytucji stać na samodzielne przygotowanie odpowiednich rozwiązań organizacyjnych i wynikających z nich rozwiązań technicznych. Należy pamiętać, że za wprowadzanie do realizacji zapisów wszystkich aktów prawnych i normatywnych odpowiedzialne jest naczelne kierownictwo, co jednak przy prawidłowo skonstruowanym systemie bezpieczeństwa nie zwalnia z odpowiedzialności służbowej szeregowych pracowników. Zwolnienie takie w sposób automatyczny następuje, gdy przepisy wewnętrzne będą sprzeczne z ogólnym systemem prawa Rzeczypospolitej Polskiej, w szczególności, gdy przygotowując i utrzymując systemy bezpieczeństwa, nie uwzględnimy wyników wykonywanej systematycznie kwerendy prawnej obejmującej wszystkie obowiązujące akty mające wpływ na systemy bezpieczeństwa informacji.

**Bibliografia**

Derfert-Wolf, L., Bednarek-Michalska, B. (red.) (2000). *Zarządzanie przez jakość w bibliotece akademickiej. Bydgoszcz – Gniew, 10–13 września 2000 r.* Bydgoszcz: Stowarzyszenie Bibliotekarzy Polskich, KWE. Pobrano 28 lutego 2015 roku z: http://www.ebib.pl/publikacje/matkonf/atr/indexpl.html

Koziara, A., Magiera, E. (2005). Model centralnego projektowania i wdrażania systemów informatycznych wspomagających proces działania państwowych szkół wyższych. W: A. Nowakowski (red.), *Infobazy'2005 - bazy danych dla nauki : materiały konferencji, Gdańsk, 25-27 września 2005* (s. 262–267). Gdańsk: Centrum Informatyczne TASK.

(Rozporządzenie, 2004). Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. 2004, nr 100, poz. 1024).

(Rozporządzenie, 2012). Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. (Dz.U. 2014, poz. 1671).

(Ustawa, 1997a). Ustawa z dnia 27 czerwca 1997 r. o bibliotekach z późn. zm.; tekst jednolity na dzień 22 maja 2012 r. (Dz.U. 2012, poz. 642).

(Ustawa, 1997b). Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych z późn. zm.; tekst jednolity na dzień 26 czerwca 2014 r. (Dz.U. 2014, poz. 1182).

(Ustawa, 2001). Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych z późn. zm. (Dz.U. 2001, nr 128, poz.1402).

(Ustawa, 2005). Ustawa z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym z późn. zm.; tekst jednolity na dzień 9 października 2013 r. (Dz.U. 2014, poz. 1198).

**Andrzej Koziara, Agnieszka Jezierska**

***Security of data and IT systems in libraries. Overview of the legal status***

**Summary**

Proper operation of the IT systems requires actions that allow their proper preparation and further use. These processes are based on international and national regulations. In terms of legal regulations, the paper presents bills, acts and regulations approved by the European Parliament, the Parliament (Sejm) of the Republic of Poland as well as the Council of Ministers. The article also describes the obligations and analyzes the actions undertaken by the University of Silesia as a result of those decisions. The presentation concerning international standards, regards issues associated with providing quality and security of ICT systems as the technological basis of the contemporary IT systems. The author presents documents regarding risk analysis and action in case of emergency situations, as well as theoretical studies, published as common documents, i.e. PN-ISO/IEC, ISO family or standard technical reports. A comparative analysis of documents is presented, especially in terms of common elements which have impact on practical solutions.

**Keywords:** ICT security, Information systems security, modern scientific libraries